Technická univerzita v Liberci

FAKULTA PŘÍRODOVĚDNĚ-HUMANITNÍ A PEDAGOGICKÁ

Katedra: Katedra aplikované matematiky

Studijní program: Specializace v pedagogice

Studijní obor: Anglický jazyk se zaměřením na vzdělávání/Informatika se zaměřením na vzdělávání

VYBRANÉ METODY STŘEDOŠKOLSKÉ MATEMATIKY V KRYPTOGRAFII

SELECTED METHODS OF SECONDARY MATHEMATICS IN CRYPTOGRAPHY

Bakalářská práce: 11-FP-KAPi-001

Autor:

Jaroslav DVOŘÁK

Podpis:

.....

Vedoucí práce: Doc. RNDr. Miroslav Koucký, CSc.

Konzultant:

Počet

stran	grafů	obrázků	tabulek	pramenů	příloh
51	0	3	10	8	3

V Liberci dne: 29. 4. 2011

Originál zadání práce

Čestné prohlášení

Název práce: Vybrané metody středoškolské matematiky v kryptografii
Jméno a příjmení autora: Jaroslav Dvořák
Osobní číslo: P07000265

Byl/a jsem seznámen/a s tím, že na mou bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, zejména § 60 – školní dílo.

Prohlašuji, že má bakalářská práce je ve smyslu autorského zákona výhradně mým autorským dílem.

Beru na vědomí, že Technická univerzita v Liberci (TUL) nezasahuje do mých autorských práv užitím mé bakalářské práce pro vnitřní potřebu TUL.

Užiji-li bakalářskou práci nebo poskytnu-li licenci k jejímu využití, jsem si vědom povinnosti informovat o této skutečnosti TUL; v tomto případě má TUL právo ode mne požadovat úhradu nákladů, které vynaložila na vytvoření díla, až do jejich skutečné výše.

Bakalářskou práci jsem vypracoval/a samostatně s použitím uvedené literatury a na základě konzultací s vedoucím bakalářské práce a konzultantem.

Prohlašuji, že jsem do informačního systému STAG vložil/a elektronickou verzi mé bakalářské práce, která je identická s tištěnou verzí předkládanou k obhajobě a uvedl/a jsem všechny systémem požadované informace pravdivě.

V Liberci dne: 29. 4. 2011

.....

Jaroslav Dvořák

Poděkování

Děkuji vedoucímu mé práce Doc. RNDr. Miroslavu Kouckému, CSc. za to, že mi dal možnost na tomto tématu pracovat, za poutavé přednášky a semináře i za jeho cenné rady. Zároveň děkuji své rodině za vytrvalou podporu.

Anotace

Tato bakalářská práce na téma „Vybrané metody středoškolské matematiky v kryptografii“ je zaměřena na studium základů teorie dělitelnosti a na jejich využití v kryptografii. Po vymezení několika základních pojmů je teorii dělitelnosti a prvočíslům věnována hlavní pozornost, protože se v zásadě jedná o jednoduché výsledky i metody, které se vyučují na střední škole a zároveň jde o velmi účinné metody, na kterých je postavena celá řada kryptografických systémů. Cílem této práce je studium algoritmů šifer především po stránce matematické, jež by případnému čtenáři mohlo napomoci nejen s výukou informatiky, ale také zejména s výukou základních matematických pojmů na střední škole.

Klíčová slova: kryptografie, šifra, teorie dělitelnosti, NSD, prvočíslo, modulo.

Annotation

This bachelor thesis entitled „Selected methods of secondary mathematics in cryptography“ is focused on studying the fundamentals of the theory of divisibility and their use in cryptography. Having defined several basic concepts is the theory of divisibility and prime numbers given major attention, because these are basically simple counts and methods that are taught at secondary schools and also as a very effective method are used as a wide range of cryptographic systems. The aim of this work is to study the cipher algorithms especially in terms of mathematics, which could help to a reader not only with teaching informatics, but also and especially in teaching basic mathematical concepts at secondary schools.

Keywords: cryptography, cipher, the theory of divisibility, GCD, prime number, modulo.

Die Annotation

Diese Bakkalaureatsarbeit mit dem Titel „Die ausgewählte Methoden der Mittelschulmathematik in der Kryptographie“ ist konzentriert auf das Studium der Fundamenten der Theorie der Teilbarkeit und ihre Verwendung in der Kryptographie. Nach der Definition einigen grundlegenden Konzepte ist die Theorie der Teilbarkeit und den Primzahlen eine große Aufmerksamkeit geschenkt, da im Grunde um die einfache Ergebnisse und Methoden geht, die an der Mittelschulen unterrichtet sind und zugleich geht es um sehr effektive Methoden, auf denen die ganze Reihe den kryptographischen Systemen gegründet sind. Das Ziel dieser Arbeit ist die Untersuchung der Verschlüsselungsalgorithmen vor allem in dem Bezug auf die Mathematik, die dem eventuellen Leser nicht nur mit dem Informatikunterricht, aber auch besonders mit dem Unterricht der grundlegenden mathematischen Begriffen auf der Mittelschule helfen könnte.

Die Schlüsselwörter: die Kryptographie, die Verschlüsselung, die Theorie der Teilbarkeit, ggT , die Primzahl, der Modulo.

Obsah

Seznam použitého značení

Množiny

N	… množina všech přirozených čísel $N = \{0, 1, 2, \ldots\}$,
N^+	… množina kladných přirozených čísel $N^+ = \{1, 2, 3, \ldots\}$,
Z	… množina všech celých čísel $Z = \{\ldots -2, -1, 0, 1, 2, \ldots\}$,
$x \in N$	… x je prvkem množiny N,
$(x_1, \ldots, x_n)$	… uspořádaná n-tice prvků,
$X_1 \times \ldots \times X_n$	… kartézský součin množin $X_1, \ldots, X_n$,
$\lvert S \rvert$	... počet prvků množiny s (mohutnost, kardinalita).

Dělitelnost

$NSD(x,y)$	… největší společný dělitel čísel x a y;
$NSN(x,y)$	… nejmenší společný násobek x a y;
$x \mid y$	... x dělí beze zbytku y,
$x \nmid y$	... x nedělí beze zbytku y,
$x \equiv y \bmod(m)$	… x je kongruentní s y modulo m,
$x \not\equiv y \bmod(m)$	… x není kongruentní s y modulo m,
$x = (y \bmod m)$	… x je zbytkem při dělení y číslem m.

Funkce

$n!$	… n faktoriál,
$\varphi(n)$	… hodnota Eulerovy funkce v bodě n.

Kryptologie

d	… dešifrovací klíč,
e	… šifrovací klíč,
k_s	… soukromý klíč,
k_v	… veřejný klíč,
A	… abeceda,
C	… prostor zašifrovaných textů,
K	… prostor klíčů,
M	… prostor otevřených textů.

1 Úvod

1.1 Význam šifer

Ačkoliv kryptografie již zdaleka není pouze nástrojem králů, generálů či spiklenců a jejích služeb využíváme téměř všichni, zůstává tento vědní obor stále mimo povědomí naší společnosti. Vůči kryptografii toto není příliš korektní, vezmeme-li v úvahu, že kryptografie provází člověka již více než dva a půl tisíce let, během nichž na ní závisel nejeden lidský život, někdy i životy celých národů. Převážně v dnešní době masivního rozvoje internetu je nutnost střežit bezpečnost citlivých informací velmi důležitá.

V historii existuje mnoho šifer, které už sice dnes, v době, kdy na ně můžeme útočit metodou hrubé síly, nemají praktické využití, dobře však ilustrují vývoj a matematické metody, které lze k šifrování či dešifrování aplikovat. A právě implementace některých významných šifer z období klasické kryptografie a studium matematických metod je tématem následující bakalářské práce.

1.2 Historická poznámka

Historie kryptografie pravděpodobně začala v 7.–6. století př. n. l., kdy hebrejští písaři použili při psaní Hebrejské bible zvláštní zápis pro některá jména a názvy. Jejich šifrovací systém byl založen na jednoduchém principu, že první písmeno abecedy nahrazovali posledním, druhé předposledním atd. čímž vytvořili nejstarší známou šifru, zvanou Abtaš.

Zhruba o 200 let později kryptografie odstartovala svůj vliv v celosvětovém měřítku. Pro vojenské účely ji totiž objevili spartští vojáci, kteří pro přenos zpráv používali šifry založené na transpozici písmen, takzvaný Skytale. Tajemství spočívalo v dřevěné tyči, kolem níž se namotal proužek kůže tak, aby pokryl povrch tyče. Poté na něj byla zapsána zpráva ve směru podélné osy. Po odmotání proužku byla zpráva nečitelná. Jak dalece dopomohla Sparťanům tato technika ochrany informací před neautorizovaným přístupem k vítězství, už asi nezjistíme, nicméně postupem času se

síla použitého kryptovacího systému stala jedním z rozhodujících faktorů téměř každého válečného konfliktu.

Promyšlený systém šifrování textu na jedné straně a schopnost tuto šifru dešifrovat na druhé straně rozhodly i o osudu anglické královny Alžběty. V roce 1586 spiklenecká skupina v čele se sirem Anthonym Babingtonem a skotskou královnou Marií Stuartovnou intrikovala prostřednictvím šifrových zpráv tak, že ačkoliv byly zachytávány královninými informátory, nebylo z nich možné nic zjistit. Působily totiž jako pouhá změť znaků. Systém této šifry byl důmyslný, nebyly pouze převedeny jednotlivé znaky na jiné, ale také jednotlivá nejfrekventovanější slova a fráze měla zástupné symboly. Sir Francis Walsingham a jeho spolupracovníci ji přeci jen prolomili, čímž zabránili nejen vraždě královny Alžběty, ale i invazi Španělů na ostrovy, která také byla v Babingtonově plánu.

Vstup Američanů do první světové války byl taktéž ovlivněn kryptografií. Angličané zachytili a dešifrovali telegram mířící z Německa do Mexika, ve kterém žádali Němci Mexiko o vytvoření spojenectví proti dosud neutrálním Američanům. Tato zpráva zbudila ve Spojených státech velké rozhořčení a následně vyhlásili Německu válku, a pomohla tak uspíšit konec celosvětového konfliktu.

Je zřejmé, že ač se kryptograf patrně hned tak nedočká podobné společenské prestiže, jaké se dostává třeba matematikům či fyzikům, může ho těšit pocit, že to byli v historii často právě kryptografové, kdo určoval chod dějin. A jsou to možná i tyto příběhy z minulosti, které dělají z kryptografie tak lákavý studijní obor. [1]

1.2.1 Steganografie

Utajená komunikace pomocí ukrytí zprávy se nazývá steganografie podle řeckých slov steganos (schovaný) a graphein (psát). Herodotos vypráví příběh, v němž vystupuje Histiaios, který chtěl podnítit Aristagora ke vzpouře proti perskému králi. K bezpečnému zaslání zprávy oholil Histiaios hlavu svého posla, napsal zprávu na lebku a až poslovi znovu narostly vlasy, poslal ho bez potíží až k příjemci zprávy.

Od té doby se v různých částech světa rozvinuly rozmanité formy steganografie. Například Číňané psali zprávy na jemné hedvábí, které pak zmačkali do malé kuličky a zalili ji voskem. Posel poté musel voskovou kuličku spolknout. Jinde zase italský vědec Giovanni Porta v 16. století popsal, jak ukrýt zprávu ve vejci vařeném natvrdo pomocí

inkoustu vyrobeného z kamence a octa. Tím se napíše zpráva na skořápku, roztok se vsaje póry a zanechá zprávu na vařeném bílku. Zprávu lze odhalit oloupáním vajíčka.

Do steganografie patří i další neviditelné inkousty, které jsou známy z návodů Plinia Staršího již z 1. století našeho letopočtu. Jde například o použití mléka pryšce jako neviditelný inkoust. Mléko je po zaschnutí naprosto průhledné, když se ale mírně zahřeje, zhnědne. Dokonce moderní špioni někdy nahrazovali vlastní močí neviditelný inkoust, když jim došel.

Dlouhá tradice steganografie jasně ukazuje, že jde o techniku, jež sice poskytuje určitý stupeň utajení, avšak má jednu zásadní vadu a to, že se objevená zpráva prozradí naráz, což znamená ztrátu veškerého utajení. [1]

1.2.2 Kryptografie

Současně se steganografií se začala rozvíjet i kryptografie, jejíž etymologie je z řeckého slova *kryptos* (skrytý). Kryptograf je člověk, který se zabývá šifrováním zpráv. Kryptografie není zaměřená na utajování zpráv, nýbrž na skrytí jejího významu a to pomocí šifrování. Zprávu lze šifrovat podle předem domluvených pravidel mezi příjemcem a odesilatelem. Bez znalostí těchto pravidel je zpráva pro nepřítele nečitelná.

Ačkoliv kryptografie a steganografie jsou dvě různé nezávislé techniky, z důvodu větší bezpečnosti zprávy je možné je kombinovat. Příkladem mohou být mikrotečky, které se používaly zejména během druhé světové války. Němečtí agenti v Latinské Americe zmenšili fotografickou cestou celou stránku textu do velikosti tečky na konci věty a tu pak umístili do nevinného dopisu. FBI se podařilo zachytit první mikrotečku díky tipu – hledat jemný odlesk filmového materiálu.

Od té doby bylo možné číst obsah mikroteček. Jestliže Němci zprávu před zmenšením zašifrovali, zabránili tak i jejímu vyzrazení. Američané tak mohli německou komunikaci sledovat, případně narušovat, avšak žádné informace o německých špionážních aktivitách nebyly získány. Účinnost kryptografie je mnohonásobně vyšší než steganografie, neboť s její pomocí je možné zabránit padnutí utajované informace do rukou nepřítele. [1]

1.2.3 Kryptoanalýza

Kryptoanalýza je prakticky opak kryptografie. Kryptografové se snaží zprávu ochránit před neautorizovaným přítupem a kryptoanalytici se snaží prolomit šifru a získat tak otevřený text bez znalosti klíče. Jednou z kryptoanalytických metod, která prolomí většinu klasických šifer, je frekvenční analýza. Frekvenční analýza funguje na základě sledování relativní četnosti jednotlivých písmen v určitém jazyce. Následně pak sleduje četnost znaků v šifrovém textu. Tuto techniku nelze používat zcela mechanicky, protože relativní četnost písmen představuje průměr a zcela přesně neodpovídá poměrům v každém textu. [1]

Kryptoanalýza studuje způsoby, postupy a možnosti prolomení šifrovacího mechanismu, zatímco *kryptografie* (šifrování) je vědní obor zabývající se studiem možností převodu zpráv do podoby, která je pro ostatní čitelná jen se znalostí šifrovacího klíče. *Kryptologie* jako vědní obor je množina zastřešující kryptografii a kryptoanalýzu. Kryptologie se zabývá šifrováním ze všech úhlů pohledu.

2 Matematika na pozadí šifrování

Zásadní význam má v oblasti šifrování teorie dělitelnosti, která odkrývá vlastnosti celých čísel vzhledem k operaci dělení. V této kapitole budeme pracovat v oboru celých čísel, která budeme značit *Z*, resp. v oboru přirozených čísel *N*. Celá čísla tvoří algebraickou strukturu, která je uzavřena vzhledem k operacím sčítání, odčítání a násobení (tj. součet, rozdíl i součin libovolných dvou celých čísel je opět celé číslo), ale není uzavřena vzhledem k operaci dělení.

2.1 Úvod do teorie dělitelnosti

Definice (relace „býti dělitelem“): Pro $x, y \in Z$ $(x \neq 0)$ říkáme, že x dělí y (beze zbytku), píšeme $x|y$, právě když existuje $q \in Z$ tak, že $y = q \cdot x$.

Poznámka:

- V případě, kdy $x|y$, říkáme, že x je dělitelem y, resp. y je násobkem x. Vlastnost, kdy x nedělí y, zapisujeme $x \nmid y$.
- Pokud $x|y$ a $x \neq \pm 1$ a $x \neq \pm y$ říkáme, že x je vlastní dělitel čísla y. Dělitele $\pm 1, \pm y$ označujeme jako nevlastní dělitele čísla y.
- V další části budeme z důvodu přehlednosti uvažovat pouze kladné dělitele.

Pro následující úvahy má zásadní význam všeobecně známé tvrzení, označované jako věta o dělení se zbytkem.

Tvrzení (dělení se zbytkem): Je-li $x \in N$ a $y \in Z$, pak existuje jediné celé číslo $q \in Z$, tzv. neúplný podíl a přirozené číslo $r \in N$, tzv. zbytek, tak, že

$y = q \cdot x + r$, kde $0 \leq r < x$. [4]

2.2 Společný dělitel a násobek

Mezi základní pojmy teorie dělitelnosti, se kterými budeme dále pracovat patří společný dělitel, největší společný dělitel, společný násobek a nejmenší společný násobek. Jde o pojmy, se kterými se studenti seznamují a pracují i v běžných hodinách matematiky.

2.2.1 Společný dělitel, největší společný dělitel

Definice (společný dělitel): Nechť $x, y \in Z$. Přirozené číslo $d \in N^+$ nazveme společným dělitelem čísel x a y, jestliže $d \mid x$ a současně $d \mid y$.

Poznámka: V souladu s dříve uvedenou definicí vyšetřujeme pouze kladné společné dělitele.

Definice (největší společný dělitel): Jestliže $x, y \in Z$ a zároveň alespoň jedno z čísel x, y je různé od nuly, pak největším společným dělitelem čísel x, y rozumíme takového jejich společného dělitele, který je největší ze všech společných dělitelů. Největšího společného dělitele budeme značit $NSD(x,y)$.

Poznámka:

- Pro libovolná $x, y \in Z - \{0\}$ existuje největší společný dělitel vždy a je určen jednoznačně.
- Řekneme, že čísla $x, y \in Z$ jsou nesoudělná, jestliže jejich největší společný dělitel je roven jedné, tj. $NSD(x,y) = 1$. [4]

Příklad 2.1

Čísla $x = 3\,456$, $y = 7\,248$ mají následující společné dělitele 1, 2, 3, 4, 6, 8, 12, 16, 24, 48 a tudíž $NSD(x,y) = 48$.

Čísla $x = 1\,234$, $y = 4\,321$ mají pouze jediného společného dělitele 1, tudíž jsou nesoudělná.

Eukleidův algoritmus

je postup, kterým lze určit největšího společného dělitele dvou přirozených čísel. Tento algoritmus spočívá v opakované aplikaci výše uvedené věty o dělení se zbytkem a může být popsán následovně:

Nechť $a, b \in N^+$ jsou čísla, jejichž největšího společného dělitele hledáme, potom

$$\begin{aligned}
a &= b \cdot q_0 + r_1, & 0 < r_1 < b,\\
b &= r_1 \cdot q_1 + r_2, & 0 < r_2 < r_1,\\
r_1 &= r_2 \cdot q_2 + r_3, & 0 < r_3 < r_2,\\
&\vdots & \vdots\\
r_i &= r_{i+1} \cdot q_{i+1} + r_{i+2}, & 0 < r_{i+2} < r_{i+1},\\
&\vdots & \vdots\\
r_{n-2} &= r_{n-1} \cdot q_{n-1} + r_n, & 0 < r_n < r_{n-1},\\
r_{n-1} &= r_n \cdot q_n.
\end{aligned}$$

Největší společný dělitel čísel *a*, *b* je poslední od nuly různý zbytek, tzn. $NSD(a,b) = r_n$. [4]

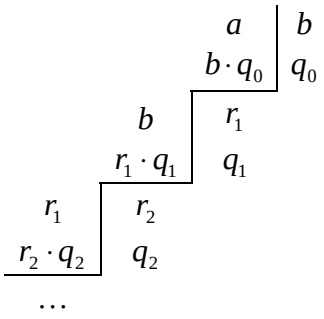
Příklad 2.2

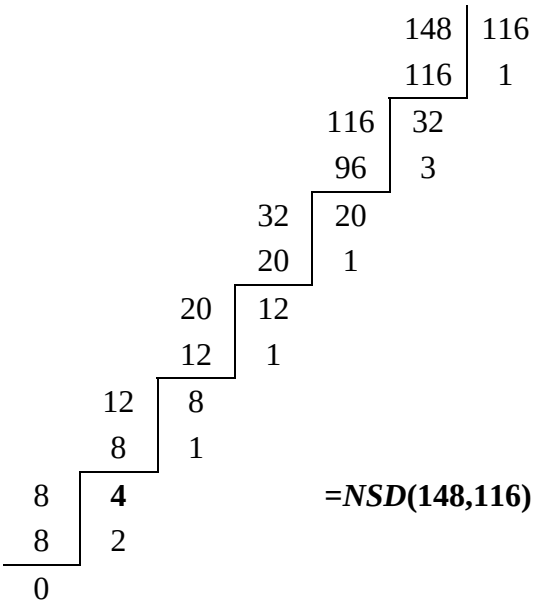
Nalezení *NSD*(148,116) pomocí Eukleidova algoritmu

r_i	r_{i+1}	r_{i+2} (zbytek)	$r_i = r_{i+1} \cdot q_{i+1} + r_{i+2}$
148	116	32	148 = 116 · 1 + 32
116	32	20	116 = 32 · 3 + 20
32	20	12	32 = 20 · 1 + 12
20	12	8	20 = 12 · 1 + 8
12	8	4	12 = 8 · 1 + 4
8	4	0	8 = 4 · 2 + 0
4	0		konec algoritmu

Největším společným dělitelem čísel 148 a 116 je číslo 4.

V praxi se osvědčilo zapisovat Eukleidův algoritmus například pomocí následujícího schématu:





2.2.2 Společný násobek, nejmenší společný násobek

Definice (společný násobek): Nechť $x, y \in Z - \{0\}$. Přirozené číslo $D \in N^+$ nazveme společným násobkem čísel *x*, *y*, jestliže $x \mid D$ a současně $y \mid D$.

Poznámka: V souladu s výše uvedenou definicí vyšetřujeme pouze kladné společné násobky.

Definice (nejmenší společný násobek): Nejmenším společným násobkem přirozených čísel $x, y \in Z - \{0\}$ rozumíme takový jejich společný násobek, který je ze všech jejich společných násobků nejmenší. Značíme ho *NSN*(*x*,*y*).

Poznámka:

- Pro libovolná $x, y \in Z - \{0\}$ existuje nejmenší společný násobek vždy a je určen jednoznačně.
- Součin největšího společného dělitele a nejmenšího společného násobku dvou kladných přirozených čísel se rovná součinu těchto dvou čísel, tj.
  $x \cdot y = NSD(x, y) \cdot NSN(x, y)$.
- *NSN* se využívá například při sčítání zlomků o různých jmenovatelích. [4]

2.3 Prvočísla a prvočíselné rozklady

Z hlediska dělitelnosti mají specifické postavení čísla, která jsou označovaná jako prvočísla. Jak bude vidět později, nacházejí prvočísla velké využití i v šifrování.

Definice (prvočíslo): Přirozené číslo větší než 1, které má pouze nevlastní dělitele, tj. je dělitelné pouze číslem 1 a samo sebou, se nazývá **prvočíslo**. Přirozené číslo větší než 1, které není prvočíslem, se nazývá **složené číslo**.

Tvrzení (Eukleides): Existuje nekonečně mnoho prvočísel.

Tvrzení (Základní věta aritmetiky): Každé přirozené číslo větší než jedna lze rozložit na součin prvočísel a to jednoznačně, pokud nepřihlížíme k pořadí prvočísel.

Jako důsledek předchozího tvrzení dostáváme, že každé přirozené číslo $x > 1$ lze jednoznačně vyjádřit ve tvaru kanonického rozkladu, který má tvar

$$x = p_1^{s_1} \cdot p_2^{s_2} \cdot \ldots \cdot p_n^{s_n},$$

kde $p_1, p_2, \ldots, p_n$ jsou různá prvočísla seřazená vzestupně, tj. $p_1 < p_2 < \ldots < p_n$. Exponenty $s_i \in N^+$ vyjadřují tzv. násobnost prvočísla p_i. Použití najdeme např. ve výše zmíněném hledání *NSD* a *NSN*.

Největšího společného dělitele lze určit prostřednictvím kanonických rozkladů obou čísel. Jsou-li *x*, *y* přirozená čísla s kanonickými rozklady

$$x = p_1^{s_1} \cdot p_2^{s_2} \cdot \ldots \cdot p_n^{s_n},$$

$$y = q_1^{r_1} \cdot q_2^{r_2} \cdot \ldots \cdot q_m^{r_m},$$

potom největší společný dělitel má tvar

$$NSD(x, y) = u_1^{t_1} \cdot u_2^{t_2} \cdot \ldots \cdot u_k^{t_k}$$

tj. zahrnuje všechna prvočísla $u_1, u_2, ..., u_k$, která se vyskytují zároveň v obou prvočíselných rozkladech a u každého použijeme **minimální** mocninu, ve které se vyskytuje. [4]

Tento výpočet je snadný, pokud známe kanonické rozklady čísel *x* a *y*. V praxi je však obtížně použitelný s výjimkou malých čísel, neboť získání kanonických rozkladů je extrémně náročná operace. Pro praktické výpočty slouží výrazně rychlejší algoritmy, zejména tzv. Eukleidův algoritmus.

Příklad 2.3

Nalezení *NSD*(148,116) pomocí kanonických rozkladů.

$$148 = 2^2 \cdot 37$$

$$116 = 2^2 \cdot 29$$

$$NSD(148,116) = 2^2 = 4$$

Nejmenší společný násobek dvou čísel lze určit prostřednictvím kanonických rozkladů obou čísel

$$x = p_1^{s_1} \cdot p_2^{s_2} \cdot \ldots \cdot p_n^{s_n},$$

$$y = q_1^{r_1} \cdot q_2^{r_2} \cdot \ldots \cdot q_m^{r_m},$$

potom nejmenší společný násobek má tvar

$$NSN(x, y) = u_1^{t_1} \cdot u_2^{t_2} \cdot \ldots \cdot u_h^{t_h}$$

tj. zahrnuje všechna prvočísla $u_1, u_2, ..., u_h$, která se vyskytují v kanonických rozkladech (tzn. alespoň v jednom z nich) a u každého použijeme **maximální** mocninu, ve které se vyskytuje. [4]

Příklad 2.4

Nalezení *NSN*(148,116) pomocí kanonických rozkladů

$$148 = 2^2 \cdot 37, \quad 116 = 2^2 \cdot 29$$

$$NSN(148,116) = 2^2 \cdot 29 \cdot 37 = 4\,292$$

Dále snadno ověříme, že platí $NSD(x, y) \cdot NSN(x, y) = x \cdot y$

$$4 \cdot 4\,292 = 17168 = 148 \cdot 116$$

Eulerova funkce

Uvažujme kladné přirozené číslo $x \in N^+$. Pro $x > 1$ označíme symbolem $\varphi(x)$ počet přirozených čísel menších než *x*, která jsou s *x* nesoudělná. Pro $x = 1$ dodefinujeme $\varphi(1) = 1$. Zobrazení φ se nazývá Eulerova funkce.

Tvrzení: Nechť $x > 1$ je přirozené číslo s kanonickým rozkladem

$$x = p_1^{s_1} \cdot p_2^{s_2} \cdot \ldots \cdot p_n^{s_n}.$$

Potom

$$\varphi(x) = x \cdot (1 - 1/p_1) \cdot (1 - 1/p_2) \cdot (1 - 1/p_3) \cdots (1 - 1/p_n).$$

Navíc, jestliže $x, y \in N^+$ jsou dvě přirozená čísla pro která platí, že *NSD*(*x*,*y*) = 1, pak

$\varphi(x, y) = \varphi(x) \cdot \varphi(y)$. [4]

2.3.1 Řetězové zlomky

Objev řetězových zlomků byl motivován touhou mít „matematicky čistou“ reprezentaci pro reálná čísla. Uvažujme následovně. Nechť $\alpha \in R$ je reálné číslo, které není celé. Potom ho lze vyjádřit ve tvaru

$\alpha = q_0 + \frac{1}{\alpha_1}$, kde $\alpha_1 > 1$ a q_0 je celé číslo.

Jestliže α_1 není přirozené číslo, můžeme ho vyjádřit obdobně jako α, tj.

$\alpha_1 = q_1 + \frac{1}{\alpha_2}$, kde $\alpha_2 > 1$ a q_1 je přirozené číslo.

Výše zmíněné vyjádření můžeme spojit do jednoho výrazu následovně

$$\alpha = q_0 + \frac{1}{q_1 + \frac{1}{\alpha_2}}.$$

Jestliže α_2 není přirozené číslo, můžeme pokračovat obdobně i dále. V případě racionálního α pak po konečném počtu kroků dostaneme výraz, který označujeme jako rozvoj racionálního čísla α v řetězový zlomek (výraz na pravé straně rovnosti nazýváme řetězovým zlomkem)

$$\alpha = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ddots + \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}}$$

, kde $q_0 \in Z$, ostatní $q_i \in N^+, i = 1,...,n$.

Pro zjednodušení je možné řetězový zlomek zapsat následovně

$$\alpha = [q_0, q_1, q_2, ..., q_{n-1}, q_n].$$

Řetězový zlomek je prakticky modifikace Eukleidova algoritmu, kde rozvoj racionálního čísla $\alpha = \frac{a}{b}$ v řetězový zlomek tvoří právě neúplné podíly z Eukleidova algoritmu:

1) $a = b \cdot q_0 + r_1, \quad 0 < r_1 < b, \quad \alpha = \frac{a}{b} = q_0 + \frac{1}{\alpha_1}, \quad$ kde $\alpha_1 = \frac{b}{r_1} > 1,$

2) $b = r_1 \cdot q_1 + r_2, \quad 0 < r_2 < r_1, \quad \frac{b}{r_1} = q_1 + \frac{1}{\alpha_2}, \quad$ kde $\alpha_2 = \frac{r_1}{r_2} > 1,$

3) $r_1 = r_2 \cdot q_2 + r_3, \quad 0 < r_3 < r_2, \quad \frac{r_1}{r_2} = q_2 + \frac{1}{\alpha_3}, \quad$ kde $\alpha_3 = \frac{r_2}{r_3} > 1,$

$\vdots \qquad \vdots \qquad \vdots \qquad \vdots$

n) $r_{n-2} = r_{n-1} \cdot q_{n-1} + r_n, \quad 0 < r_n < r_{n-1}, \quad \frac{r_{n-2}}{r_{n-1}} = q_{n-1} + \frac{1}{\alpha_n}, \quad$ kde $\alpha_n = \frac{r_{n-1}}{r_n} > 1,$

n+1) $r_{n-1} = r_n \cdot q_n, \quad \frac{r_{n-1}}{r_n} = q_n.$

neboli $\alpha = \frac{a}{b} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ddots + \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}}$, kde $\alpha > 1$ a $q_i \in N^+, i = 1,...,n$. [4]

Poznámka:

Výraz $\delta_i = [q_0, q_1, \ldots, q_i]$ se nazývá *i*-tý přibližný zlomek. Přibližné zlomky mají následující vlastnosti:

1) Je-li $\delta_i = \frac{P_i}{Q_i}$, potom platí

$$P_i = q_i \cdot P_{i-1} + P_{i-2}, \quad \text{kde } P_{-1} = 1,\ P_0 = q_0,$$

$$Q_i = q_i \cdot Q_{i-1} + Q_{i-2}, \quad \text{kde } Q_{-1} = 0,\ Q_0 = 1.$$

2) Pro libovolné dva sousední přibližné zlomky δ_i a δ_{i-1} platí

$$\delta_i - \delta_{i-1} = \frac{(-1)^{i+1}}{Q_i \cdot Q_{i-1}}.$$

3) Přibližné zlomky jsou v základním tvaru, tj. $NSD(P_i, Q_i) = 1$. [5]

Rozvoj racionálního čísla v řetězový zlomek se obvykle zapisuje do tzv. tabulky přibližných zlomků – viz níže.

i	–1	0	1	2	...	n
q_i	——	q_0	q_1	q_2	...	q_n
P_i	1	q_0	P_1	P_2	...	P_n
Q_i	0	1	Q_1	Q_2	...	Q_n

Příklad 2.5

Tabulka přibližných zlomků pro racionální číslo $\alpha = \frac{37}{29}$ vypadá následovně.

i	–1	0	1	2	3	4	5
q_i	——	1	3	1	1	1	2
P_i	1	1	4	5	9	14	**37**
Q_i	0	1	3	4	7	11	**29**

2.4 Úvod do kongruencí

Nyní se zaměříme na koncept nazývaný kongruence, který byl vynalezen C. F. Gaussem, a který nachází široké uplatnění při šifrování. Jde o téma, které lze rozvíjet i ve středoškolské matematice.

Definice (kongruence): Nechť $m \in N - \{0,1\}$ a $a, b \in Z$. Řekneme, že a, b jsou kongruentní modulo *m*, jestliže obě čísla mají při dělení číslem *m* stejný zbytek.

Tuto skutečnost zapíšeme následovně $a \equiv b \,(\mathrm{mod}\, m)$ nebo $a \equiv b \,(m)$ a nebo $a \equiv_m b$. V případě, že čísla *a*, *b* nemají při dělení číslem *m* stejný zbytek, říkáme, že *a*, *b* jsou nekongruentní modulo *m* a píšeme např. $a \not\equiv b \,(\mathrm{mod}\, m)$.[5]

Příklad 2.6

Snadno ověříme, že $13 \equiv 34 \,(\mathrm{mod}\, 7)$, neboť čísla 13 a 34 dávají při dělení 7 zbytek 6, tzn. jsou kongruentní modulo 7.

Tvrzení: Relace kongruence má následující vlastnosti:

a) Nechť $a_1 \equiv b_1 \,(\mathrm{mod}\, m)$, $a_2 \equiv b_2 \,(\mathrm{mod}\, m)$, pak platí:

- $a_1 + a_2 \equiv b_1 + b_2 \,(\mathrm{mod}\, m)$,
- $a_1 \cdot a_2 \equiv b_1 \cdot b_2 \,(\mathrm{mod}\, m)$,
- Jestliže $d \mid NSD(a_1, b_1) \wedge NSD(d, m) = 1$, potom $\frac{a_1}{d} \equiv \frac{a_2}{d} \,(\mathrm{mod}\, m)$.

b) Vlastnosti (změna modulu):

- Jestliže $a \equiv b \pmod{m}$, potom $k \cdot a \equiv k \cdot b \pmod{k \cdot m}$, $k \in N^+$.
- Jestliže $a \equiv b \pmod{m}$, $d \mid NSD(a,b,m)$, potom $a/d \equiv b/d \pmod{m/d}$,
- Jestliže $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}$, potom $a \equiv b \pmod{NSN(m_1, m_2)}$.

2.4.1 Řešení kongruencí 1. stupně

Tvrzení: Nechť $NSD(a,m) = 1$, potom kongruence $a \cdot x \equiv b \pmod{m}$ má právě jedno řešení pro libovolné *b*.
Toto řešení je ve tvaru

$$x \equiv (-1)^n \cdot P_{n-1} \cdot b \pmod{m},$$

kde P_{n-1} je čitatel předposledního přibližného zlomku rozvoje čísla m/a v řetězový zlomek a n je počet kroků v Eukleidově algoritmu (při vlastním řešení výsledek převedeme zpravidla do soustavy nejmenších nezáporných zbytků modulo *m*).

Při řešení obecných kongruencí $a \cdot x \equiv b \pmod{m}$ (tj. bez předpokladu $NSD(a,m) = 1$) využíváme následující tvrzení.

Tvrzení: Nechť $NSD(a,m) = d \geq 2$.

1) Jestliže $d \nmid b$ potom kongruence $a \cdot x \equiv b \pmod{m}$ nemá řešení.
2) Jestliže $d \mid b$ potom kongruence $a \cdot x \equiv b \pmod{m}$ má právě d modulo m nekongruentních řešení tvaru

   $$x \equiv x_0; x_0 + m_1; x_0 + 2 \cdot m_1; \ldots; x_0 + (d-1) \cdot m_1 \pmod{m},$$

   kde x_0 je jediné řešení kongruence

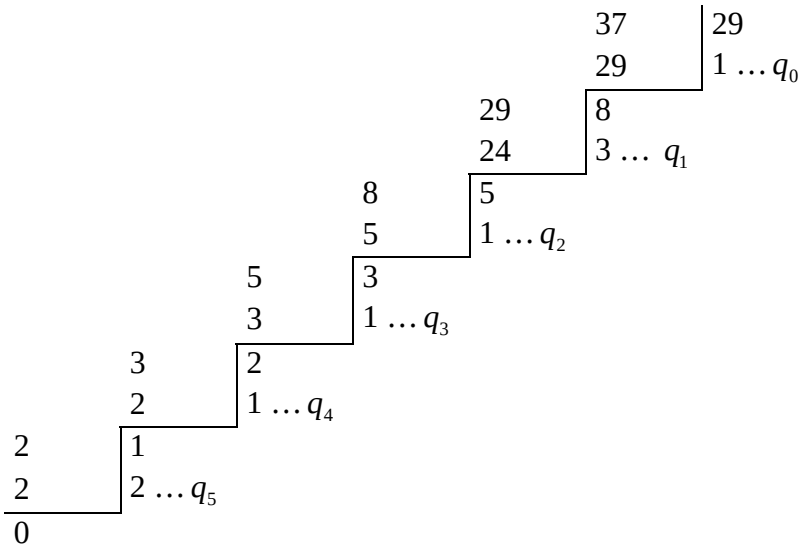
   $$a_1 \cdot x \equiv b_1 \pmod{m_1}, a_1 = a/d,\ b_1 = b/d,\ m_1 = m/d.$$ [4]

Příklad 2.7

Nalezneme všechna řešení kongruence $116x \equiv 60 \pmod{148}$.

Jelikož *NSD*(148,116) = 4 a $4 \mid 60$ má uvedená kongruence 4 řešení. Řešení původní

kongruence převedeme na řešení kongruence $29x \equiv 15 \pmod{37}$. Nalezneme hodnoty $q_0, q_1, ..., q_n$ pomocí Eukleidova algoritmu.



Do tabulky přibližných zlomku vložíme výsledky q_0 až q_5.

i	–1	0	1	2	3	4	5
q_i	——	1	3	1	1	1	2
P_i	1	1	4	5	9	14	**37**

Dosadíme do vzorce $x \equiv (-1)^n \cdot P_{n-1} \cdot b \pmod{m}$ a vypočítáme

$$x \equiv (-1)^5 \cdot 14 \cdot 15 \pmod{37}$$

$$x \equiv -210 \pmod{37}, \text{ tj. } x \equiv 12 \pmod{37}$$

Nyní jako řešení původní kongruence $116x \equiv 60 \pmod{148}$, dostaneme

$$x \equiv 12; 49; 86; 123 \pmod{148}.$$

2.5 Permutace

Definice (permutace): Je dána množina $X = \{1, 2, ..., n\}$. Vzájemně jednoznačné zobrazení π množiny *X* na sebe nazveme permutaci na množině *X*.

Permutace je jeden ze základních kombinatorických pojmů a zapisujeme ji obvykle ve tvaru $\pi = \begin{pmatrix} 1 & 2 & \cdots & n \\ \pi(1) & \pi(2) & \cdots & \pi(n) \end{pmatrix}$.

Poznámka:

- Množinu všech permutací na *n*-prvkové množině označujeme S_n a pro počet prvků platí $|S_n| = n!$.
- Na množině S_n lze definovat operaci násobení permutací (jako skládání zobrazení) následovně – je-li $\pi, \rho \in S_n$, potom součinem permutací π, ρ (v tomto pořadí) rozumíme permutaci $\pi \cdot \rho$ definovanou následovně:

  $(\pi \cdot \rho) \cdot (i) = \rho \cdot (\pi \cdot (i))$,

  neboli $\pi \cdot \rho = \begin{pmatrix} 1 & 2 & \cdots & n \\ \rho(\pi(1)) & \rho(\pi(2)) & \cdots & \rho(\pi(n)) \end{pmatrix}$.
- Inverzní permutaci k permutaci π značíme π^{-1} a definujeme vztahem $\pi \cdot \pi^{-1} = \begin{pmatrix} 12\cdots n \\ 12\cdots n \end{pmatrix}$. Pro $\pi = \begin{pmatrix} 1 & 2 & \cdots & n \\ \pi(1) & \pi(2) & \cdots & \pi(n) \end{pmatrix}$, tedy dostáváme $\pi^{-1} = \begin{pmatrix} \pi(1) & \pi(2) & \cdots & \pi(n) \\ 1 & 2 & \cdots & n \end{pmatrix}$.[4]

Příklad 2.8

Mějme dvě permutace z S_4: $\pi = \begin{pmatrix} 1\,2\,3\,4 \\ 2\,1\,4\,3 \end{pmatrix}$, $\rho = \begin{pmatrix} 1\,2\,3\,4 \\ 1\,3\,4\,2 \end{pmatrix}$.

Pak $\pi \cdot \rho = \begin{pmatrix} 1\,2\,3\,4 \\ 3\,1\,2\,4 \end{pmatrix}$, $\rho \cdot \pi = \begin{pmatrix} 1\,2\,3\,4 \\ 2\,4\,3\,1 \end{pmatrix}$ a $\pi^{-1} = \begin{pmatrix} 2\,1\,4\,3 \\ 1\,2\,3\,4 \end{pmatrix}$.

3 Úvod do kryptografie

3.1 Historická poznámka

Vytvoření šifrování s veřejným klíčem Diffie a Hellman v roce 1976 a následný vynález Rivesta, Shamira a Adlemana šifrovacího systému RSA v roce 1978 jsou zlomové okamžiky v dlouhé historii kryptografie. Je těžké nepřeceňovat důležitost šifrování s veřejným klíčem a následného schéma digitálního podpisu v moderním světě počítačů a internetu.

Nemůžeme se ihned zaměřit na ty nejnovější poznatky při studiu kryptologie, ale je nutné postupovat podle historického vývoje. Nejprve se seznámíme s některými základními pojmy v šifrování. Pak si představíme symetrické šifrování, které sloužilo jako předloha pro mnoho dalších kryptosystémů, jehož prvky můžeme nalézt i v asymetrickém šifrování, které završí šifrovací metody. V historii se používalo mnoho rozličných šifrovacích systémů, které se již v dnešní době prakticky nevyužívají, jelikož na ně můžeme útočit metodou hrubé síly, avšak výborně představují možnosti a nároky na kryptografy své doby. A právě využitím některých významných šifer se zaobírá následující část této bakalářské práce.

3.2 Základní pojmy v šifrování

Definice (otevřená abeceda): Otevřená abeceda A je množina všech znaků (číslic, písmen nebo symbolů) používaných k vytvoření nezašifrovaných zpráv.

Definice (prostor otevřených textů): Prostor otevřených textu M je množina všech potenciálně možných zpráv určených k zašifrování, tj. konečných řetězců nad otevřenou abecedou A. Formálně $M \subseteq A^*$.

Definice (šifrová abeceda): Šifrová abeceda B je množina všech znaků, které se používají k vytvoření zašifrované zprávy.

Definice (prostor zašifrovaných textů): Prostor zašifrovaných textů *C* je podmnožina množiny konečných řetězců nad šifrovou abecedou *B*, tj. $C \subseteq B^*$.

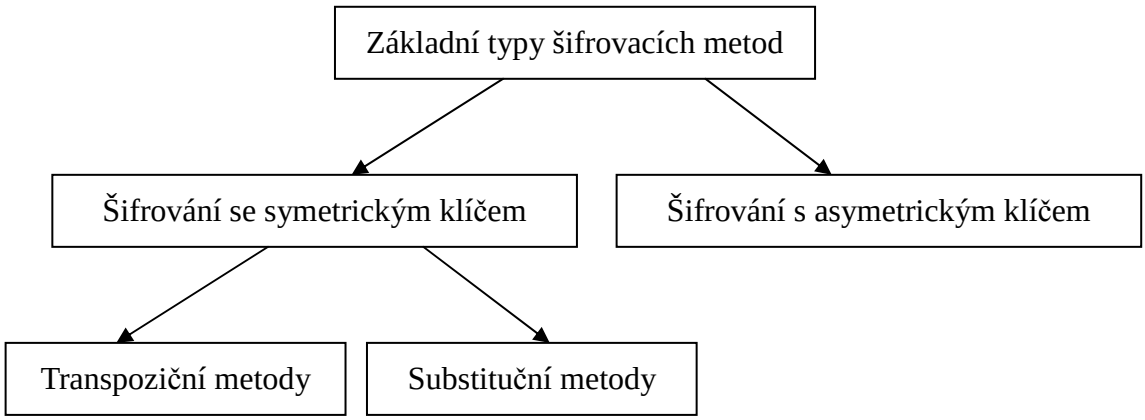
Definice (prostor klíčů): Prostor klíčů je konečná množina $K = \{k \mid k = (e,d)\}$, kde *e* je tzv. šifrovací klíč a *d* je tzv. dešifrovací klíč.

Šifrování je prosté zobrazení $E_e : M \to C$. Jde tedy o transformaci otevřeného textu $m \in M$ na zašifrovaný text $c \in C$ pomocí parametru (šifrovacího klíče) e.

Dešifrování je transformace zašifrovaného textu $c \in C$ pomocí parametru d (dešifrovací klíč příslušný k šifrovacímu klíči *e*) zpět na původní text $m \in M$. Jedná se tedy o inverzní zobrazení $D_d : C \to M$ k zobrazení E_e.
Šifrovací systém tak musí splňovat následující podmínku

$$\forall k = (e,d) \in K, \forall m \in M \text{ platí } D_d(E_e(m)) = m.$$

S ochranou dat souvisí tzv. **Kerckhoffův princip**, který lze formulovat následovně: **„bezpečnost šifrovacího systému nesmí záviset na utajení šifrovacího algoritmu, ale na utajení klíče“.** Tento princip je všeobecně uznáván, proto se tvůrci šifer soustředili na vytvoření veřejně známých šifrovacích systémů a na ověření toho, že jsou opravdu bezpečné. Takovými algoritmy jsou například symetrická šifra AES nebo hashovací funkce SHA-2. Jejichž bezpečnost se ověřila tím, že i přes mnohaletou práci vědců se nepodařilo najít dostatečně efektivní způsob, jak tyto šifry prolomit. [2] [8]



Obrázek 1: Šifrovací metody

3.3 Symetrické metody šifrování

Symetrické šifrování, které vzniklo mnohem dříve než asymetrické šifrování, je mnohem jednodušší než asymetrické šifrování. Podstatnou výhodou symetrického šifrování je relativně nízká výpočetní náročnost, jelikož jeho princip je jednodušší. U tohoto typu šifrování lze ze šifrovacího klíče snadno odvodit klíč pro dešifrování, což je zároveň jeho největší slabina. Je nutné doručit klíč k adresátovi bezpečným kanálem, aby adresát mohl zprávu dešifrovat.

V symetrickém šifrování nalezneme **transpoziční metody**, kde si znaky zachovávají identitu, ale mění svojí pozici. Příkladem mohou být různé šifrovací anagramy. Další třídou jsou **substituční šifry**, kde si znaky zachovávají pozici, ale mění svojí identitu. Caesarova šifra, afinní šifra, Vigenèrova šifra a Hillova šifra jsou příklady substitučních šifer.

Další možné dělením je na tzv. **monoalfabetické** a **polyalfabetické šifry**. Monoalfabetické šifry obsahují pouze jednu šifrovou abecedu, např. Caesarova šifra nebo jednoduchá substituční šifra. Zatímco polyalfabetické šifry používají dvě a více šifrových abeced, které se střídají podle jistých pravidel. Stejné znaky otevřeného textu mohou být proto reprezentovány různými znaky šifrového textu. Vigenèrova šifra je jedním z příkladů polyalfabetické šifry.

To vše završují **blokové** a **proudové metody**. Blokové provádějí šifrování informací po blocích (např. Feistelova šifra, Vernamova šifra), zatímco proudové šifry šifrují po bitech/bajtech (např. algoritmy RC4, FISH, SEAL, WAKE). [6]

3.3.1 Transpoziční šifry

Transpoziční šifry jsou založeny na principu změny pořadí, v jakém jsou písmena napsána. Výhodou tohoto šifrování je jednoduchost. S rostoucím počtem znaků v otevřeném textu roste i počet možností, takže dešifrovat zašifrovaný text bez znalosti použitého pravidla je téměř nemožné. Existuje mnoho forem transpozice, například různé anagramy, které se řídí předem domluvenými pravidly.

Příklad (transpozice s periodou *d*)

Šifrovací klíč tvoří permutace $\pi \in S_d$

Vlastní šifrování otevřeného textu $p_1, p_2, ..., p_d$ probíhá postupně po blocích tvořených *d* znaky a může být popsáno vztahem

$$E(p_1 p_2 \dots p_d) = p_{\pi(1)} p_{\pi(2)} \cdots p_{\pi(d)}$$

Při dešifrování se používá klíč, který tvoří inverzní permutace π^{-1} je tedy popsáno vztahem

$$D(Q_1 Q_2 \dots Q_d) = Q_{\pi^{-1}(1)} Q_{\pi^{-1}(2)} \cdots Q_{\pi^{-1}(d)}$$

Příklad 3.1

Zašifrujeme otevřený text *„symetrická šifra s periodou“* pomocí jednoduché **transpoziční šifry** s klíčem $\pi = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8 \\ 2\,4\,7\,1\,6\,8\,5\,3 \end{pmatrix}$.

Otevřený text napíšeme bez mezer vedle sebe a rozdělíme do bloků po osmi, neboť perioda klíče je $\pi \in S_8$. Poté šifrujeme podle permutace, tzn. na první pozici napíšeme druhé písmeno, na druhou čtvrté, na třetí sedmé atd. v každém bloku podle následující tabulky.

	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
Otevřený text	*s*	*y*	*m*	*e*	*t*	*r*	*i*	*c*	*k*	*a*	*s*	*i*	*f*	*r*	*a*	*s*	*p*	*e*	*r*	*i*	*o*	*d*	*o*	*u*
Šifrový text	*Y*	*E*	*I*	*S*	*R*	*C*	*T*	*M*	*A*	*I*	*A*	*K*	*R*	*S*	*F*	*S*	*E*	*I*	*O*	*P*	*D*	*U*	*O*	*R*

Následující dešifrování provedeme stejným způsobem, ale použijeme inverzní permutaci , tedy $\pi^{-1} = \begin{pmatrix} 2\,4\,7\,1\,6\,8\,5\,3 \\ 1\,2\,3\,4\,5\,6\,7\,8 \end{pmatrix}$.

Příklad 3.2

Zde je jeden velice prostý příklad **transpoziční metody**, který se nazývá šifrování podle plotu. Klíč bude dlouhý pět řádek. Chceme-li zašifrovat zprávu pomocí tohoto klíče, napíšeme ji do pěti řádků a to tak, že každé písmeno je na novém řádku, tzn. první písmeno na prvním řádku, druhé písmeno na druhém řádku atd. Šesté písmeno napíšeme opět na první řádek. Poté text zapíšeme za sebe s tím, že postupujeme po řádcích – nejprve napíšeme písmena z prvního řádku, poté z řádku druhého a tak dále.

Chceme-li zašifrovat zprávu *„sejdeme se na vlachovce“* podle pětiřádkového plotu, dostaneme:

s					*m*					–					*l*					*v*		
	e					*e*					*n*					*a*					*c*	
		j					–					*a*					*c*					*e*
			d					*s*					–					*h*				
				e					*e*					*v*					*o*			

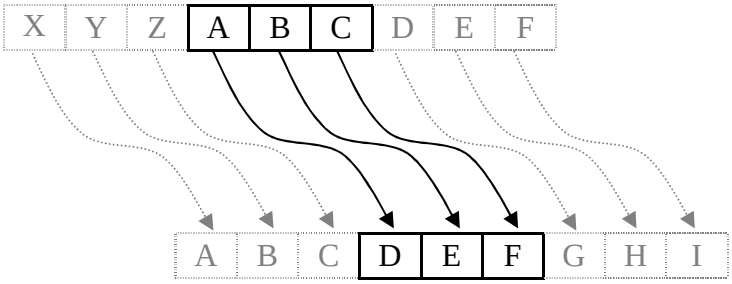
Nyní zapíšeme obsah jednotlivých řádků, čímž dostaneme následující kryptogram:

„SM LVEENACJ ACEDS HEEVO“.

Příjemce může zprávu dešifrovat tak, že proces provede v opačném pořadí.

3.3.2 Substituční šifry

Alternativou transpozičních šifer jsou šifry substituční. Jednou z nejstarších je tzv. **Caesarova šifra**, kterou popsal Julius Caesar ve svých Zápiscích o válce galské. Její princip je založen na tom, že každé písmeno je během šifrování zaměněno za písmeno, které se v abecedě nachází o tři místa dále. Ačkoliv Caesar používal posun o tři místa, stejného výsledku lze docílit použitím libovolného čísla od 1 do 25. U Caesarovy šifry je šifrovací i dešifrovací klíč definován posunem. Jakékoliv šifrování za pomoci posunu písmen tedy dnes označujeme jako Caesarovu šifru. [3]



Obrázek 2: Caesarova šifra s posunem o 3 pozice

Z pohledu kongruencí lze toto šifrování popsat vztahem

$$c \equiv (m+3) \pmod{26},$$

kde m je pořadové číslo znaku otevřeného textu a c je pořadové číslo znaku použitého k zašifrování, 3 je posunutí a 26 je počet znaků anglické abecedy. Dešifrování se pak provede posunutím o 3 pozice zpět, tj.

$$m \equiv (c-3) \pmod{26},$$

kde m je pořadové číslo znaku otevřeného textu a c je pořadové číslo zašifrovaného znaku.

Hlavní nevýhoda této šifry je její zranitelnost hrubou silou. Vzhledem k tomu, že Caesarova šifra má u běžné latinky pouze 25 možných klíčů, je tímto druhem útoku velice zranitelná. Další slabinou je, že klíč lze odvodit ze znalosti jediného páru řetězců otevřeného a šifrového textu. To je až příliš málo na to aby to bylo bezpečné.

Příklad 3.3

Aplikace Caesarovi šifry na krátkou zprávu *„I ty, můj synu?“*. Šifrový text posuneme o 3 pozice následovně (mezery v textu se vynechávají):

Otevřený text: *itymusynu*

Šifrový text: *LWBPXMVBQX*

Z hlediska kryptografické bezpečnosti je sice nezbytné mít velké množství klíčů, ale současně je třeba zdůraznit, že to samo o sobě není žádnou zárukou síly systému. Klasickou ukázkou může být **jednoduchá substituční šifra**. Rozborem této šifry zjistíme, že velké množství klíčů není žádnou zárukou neprolomitelnosti systému a navíc útočník může ke svému prospěchu využít statistiky daného jazyka – v tomto případě angličtiny.

Šifrovací klíč je tvořen permutací (viz kapitola 2.5)

$$\pi \in S_{26} \qquad \text{neboli } \pi = \begin{pmatrix} a & b & \dots & z \\ \pi(a) & \pi(b) & \dots & \pi(z) \end{pmatrix},$$

kde počet klíčů lze vyjádřit $|S_{26}| = 26! = 403\,291\,461\,126\,605\,635\,584\,000\,000$.

Dešifrovací klíč tedy je inverzní prvek

$$\pi^{-1} \in S_{26} \qquad \text{neboli } \pi^{-1} = \begin{pmatrix} \pi(a) & \pi(b) & \dots & \pi(z) \\ a & b & \dots & z \end{pmatrix}.$$

Aby bylo možné si lehce zapamatovat klíč, je dobré určit nějakou klíčovou větu, odstranit z ní všechna opakující se písmena a takto vytvořit začátek klíče, za něž se poté v abecedním pořadí zařadila veškerá zbývající písmena.

Příklad 3.4

Pro příklad **jednoduché substituční šifry** můžeme použít větu *„The fight between cryptographers and cryptoanalists is neverending.“*. Když z ní odstraníme opakující se znaky, dostaneme *„thefigbwncrypoasdlv“*. Celý klíč tedy zní:

„THEFIGBWNCRYPOASDLVJKMQUXZ“. Nejprve si napíšeme všechna písmena abecedy ve správném pořadí a pod ně poté písmena domluvené šifrové abecedy.

Otevřený text	*a*	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*j*	*k*	*l*	*m*	*n*	*o*	*p*	*q*	*r*	*s*	*t*	*u*	*v*	*w*	*x*	*y*	*z*
Šifrový text	*T*	*H*	*E*	*F*	*I*	*G*	*B*	*W*	*N*	*C*	*R*	*Y*	*P*	*O*	*A*	*S*	*D*	*L*	*V*	*J*	*K*	*M*	*Q*	*U*	*X*	*Z*

Dešifrovací klíč tvoří inverzní permutaci k permutaci, která tvoří šifrovací klíč. Šifrovacím pravidlem je nahradit každé písmeno tím, které je pod ním, dešifrovací proces je přesně opačný. Pokud bychom tedy použili jako klíč výše uvedenou tabulku, slovo *„easy“* by po zašifrování vypadalo jako *„ITVX“* a zpráva *„WTLF“* znamená ve skutečnosti *„hard“*.

Další substituční monoalfabetickou šifrou je tzv. **afinní šifra**, která částečně eliminuje zásadní nevýhodu Caesarovy šifry, která nabízela jen malý počet klíčů a tudíž i velmi primitivní kryptoanalýzu. Základem tohoto kryptografického systému je následující šifrovací funkce, kterou použiji k šifrování:

$$c = a \cdot m + b \pmod{26},$$

kde $a, b \in Z_{26}$ jsou parametry klíče a platí, že $NSD(a,26) = 1$ a kde m je pořadové číslo znaku, který šifrujeme a c je pořadové číslo zašifrovaného znaku. Pro dešifrování zprávy doporučuji upravit šifrovací funkci následujícím způsobem:

$$c = a \cdot m + b \pmod{26} \qquad \big| -b$$

$$a \cdot m = c - b \pmod{26} \qquad \big| \div a$$

$$m = a^{-1} \cdot (c - b) \pmod{26} \qquad [1]$$

Primární slabost šifry pochází z faktu, že kryptoanalytik může pomocí hrubé síly, frekvenční analýzy nebo jen odhadem objevit otevřený text a v té chvíli je ochrana dat před neautorizovaným přístupem ohrožena. [4]

Příklad 3.5

Chceme-li zašifrovat **afinní šifrou** zprávu *„tsunami“* klíčem $(a, b) = (21, 10)$ musíme

[1] Jestliže dělím a je to stejné jako když násobí a^{-1}. Vzhledem k operaci násobení je a^{-1} nazýván inverzní prvek.

nejprve převést písmena na čísla podle například tabulky pořadí znaků (viz Tabulka 2 v příloze).

Otevřený text *„tsunami“* pak bude 19, 18, 20, 13, 0, 12, 8, který postupně dosazujeme do šifrovací funkce následovně

t: $21 \cdot 19 + 10 \pmod{26} = 9 + 10 \pmod{26} = 19 \pmod{26}$,

s: $21 \cdot 18 + 10 \pmod{26} = 14 + 10 \pmod{26} = 24 \pmod{26}$,

u: $21 \cdot 20 + 10 \pmod{26} = 4 + 10 \pmod{26} = 14 \pmod{26}$,

n: $21 \cdot 13 + 10 \pmod{26} = 13 + 10 \pmod{26} = 23 \pmod{26}$,

a: $21 \cdot 0 + 10 \pmod{26} = 10 \pmod{26}$,

m: $21 \cdot 12 + 10 \pmod{26} = 18 + 10 \pmod{26} = 2 \pmod{26}$,

i: $21 \cdot 8 + 10 \pmod{26} = 12 + 10 \pmod{26} = 22 \pmod{26}$.

Šifrový text opět získáme dosazením výsledků funkcí do tabulky pořadí znaků. Tudíž čísla 19, 24, 14, 23, 10, 2, 22 převedu na písmena *„TYOXKCW“* a mohu zaslat šifrovou zprávu příjemci, který nejprve převede písmena na čísla *„TYOXKCW“* = (19, 24, 14, 23, 10, 2, 22), které dosadí do funkce $m = 21^{-1} \cdot (c - 10) \pmod{26}$, resp. $m = 5 \cdot (c - 10) \pmod{26}$ následovně

T: $5 \cdot (19 - 10) \pmod{26} = 19 \pmod{26}$,

Y: $5 \cdot (24 - 10) \pmod{26} = 18 \pmod{26}$,

O: $5 \cdot (14 - 10) \pmod{26} = 20 \pmod{26}$,

X: $5 \cdot (23 - 10) \pmod{26} = 13 \pmod{26}$,

K: $5 \cdot (10 - 10) \pmod{26} = 0 \pmod{26}$,

C: $5 \cdot (2 - 10) \pmod{26} = -40 \pmod{26} = 12 \pmod{26}$,

W: $5 \cdot (22 - 10) \pmod{26} = 8 \pmod{26}$.

Příjemce zprávy opět převede výsledky na písmena a získá tak otevřený text.

Doposud jsme řešili pouze monoalfabetické šifry. **Vigenèrova šifra** je pravděpodobně nejznámější „manuální“ polyalfabetickou šifrou. Své jméno nese po Blaisovi de Vigenèrovi, francouzském diplomatovi ze 16. století. Ačkoliv byl její koncept publikován již roku 1586, širšího využití se dočkala o 200 let později a prolomit se ji podařilo až Babbagovi a Kasiskému v polovině 19. století. Za zmínku jistě stojí, že Vigenèrovu šifru používala konfederační armáda v Americké občanské válce. Ta ovšem propukla až poté, co byla tato šifra prolomena. Vigenèrova šifra používá k šifrování tzv. Vigenèrův čtverec (viz Tabulka 1 v příloze). První sloupec

(klíčový sloupec) a první řada (písmena otevřené abecedy) obsahují anglickou abecedu. Každé písmeno otevřeného textu má svou vlastní řadu, v níž je taktéž celá abeceda, ale je posunuta v závislosti na klíčovém znaku v prvním sloupci. Tudíž každé písmeno v levém sloupci tvoří Caesarovu šifru, jejíž posun je určen právě tímto písmenem. Například u písmene f je Caesarova šifra s posunem o 5 pozic.

Z pohledu kongruencí lze toto kódování popsat vztahem

$$c \equiv (m + k_i) \pmod{26},$$

kde m je pořadové číslo původního znaku a c je pořadové číslo zašifrovaného znaku, k_i je posunutí a 26 je počet znaků anglické abecedy. Dekódování se pak provede posunutím o k_i pozice zpět, tj.

$$m \equiv (c - k_i) \pmod{26},$$

kde m je pořadové číslo původního znaku a c je pořadové číslo zašifrovaného znaku.

Vigenèrova šifra je jedním z příkladů polyalfabetických šifer, u nichž se opakovaně používá (krátká) sekvence jednoduchých substitučních šifer s pevně danou rotací. U výše představené Vigenèrovi šifry je perioda shodná s délkou klíčového slova. Jedním z důvodů pro používání polyalfabetických šifer je snaha zamaskovat četnost výskytu jednotlivých písmen v daném jazyce. [1] [2]

Příklad 3.6

Jedna z nejběžnějších metod použití **Vigenèrova čtverce** k šifrování je zvolit si klíčové slovo (nebo větu), ve které se neopakují žádná písmena. Jestliže je otevřený text delší než klíčové slovo, opakuje se klíč, tak dlouho, jak je zapotřebí, abychom vytvořili řetězec stejně dlouhý jako původní zpráva. Ten si také pod zprávu zapíšeme. Zkusíme-li na zašifrovat krátkou zprávu *„diplomat or cryptographer“* klíčovým slovem *„paris“*. Nejprve napíšeme opakovaně heslo nad text zprávy tak, abychom ji pokryli celou. Dále šifrujeme následujícím způsobem: k zašifrování prvního písmene, jímž je *d*, se nejprve podíváme, jaké písmeno klíče se u něj nachází. Je to *p*, čímž je dán řádek Vigenèrova čtverce, jenž začíná právě písmenem *P*. V průsečíku sloupce označeného *d* a řádku označeného *P* najdeme písmeno *S*, což je první písmeno hledaného šifrového textu. Pro zašifrování dalšího písmene zprávy, celý proces zopakujeme.

Každé písmeno klíčového slova indikuje konkrétní šifrovou abecedu uvnitř Vigenèrova čtverce, a protože naše heslo je složeno z pěti písmen, odesilatel šifruje za neustálého střídání pěti šifrových abeced. Páté písmeno zprávy šifrujeme přes páté písmeno klíčového slova, jímž je *s*, ale u šestého písmene se vracíme k prvnímu písmenu klíčového slova. Delší klíčové slovo nebo fráze znamená, že se používá více šifrových abeced a složitost šifry roste.

Klíčové slovo	*p*	*a*	*r*	*i*	*s*	*p*	*a*	*r*	*i*	*s*	*p*	*a*	*r*	*i*	*s*	*p*	*a*	*r*	*i*	*s*	*p*	*a*	*r*
Otevřený text	*d*	*i*	*p*	*l*	*o*	*m*	*a*	*t*	*o*	*r*	*c*	*r*	*y*	*p*	*t*	*o*	*g*	*r*	*a*	*p*	*h*	*e*	*r*
Šifrový text	*S*	*I*	*G*	*T*	*G*	*B*	*A*	*K*	*W*	*J*	*R*	*R*	*P*	*X*	*L*	*D*	*G*	*I*	*I*	*H*	*W*	*E*	*I*

Další polyalfabetická šifra, se kterou se můžeme setkat v klasické kryptografii, je **Hillovo šifrování**, kterou navrhl v roce 1929 Lester S. Hill. Tato šifra vyžaduje znalost matic a byla implementována v podobě stroje s ozubenými koly a řetězy. Zašifrovanou zprávu pomocí této metody je již obtížnější prolomit. Klíč je tvořen maticí. V prvním kroku převedeme písmena do číselné podoby (viz Tabulka 2 v příloze). Na rozdíl od předchozích typů zde šifrujeme vždy *d* po sobě jdoucích čísel najednou pomocí následující funkce

$$Y = x \cdot H ,$$

kde je klíč $H = (h_{ij})_{i,j=1}^{d}$, kde $h_{ij} \in Z_{26}$, $d \geq 2$, navíc $NSD(\det H, 26) = 1$.

Následné dešifrování je složitější. Musíme provést inverzi k provedené operaci – k násobení matic. Respektive, zprávu opět rozdělíme na bloky *d* písmen, které násobíme inverzní maticí H^{-1} k šifrové matici *H*.

Jestliže jsme získali inverzní matici dešifrujeme stejným způsobem jako jsme šifrovali, tj. podle funkce:

$$Y \cdot H^{-1} = x . \text{ [4]}$$

Příklad 3.7

Zašifrujeme text *„matrix“* pomocí **Hillova šifrování** s klíčem $H = \begin{pmatrix} 11 & 6 \\ 3 & 7 \end{pmatrix}$. Nejprve nahradíme písmena jejich pořadím, tudíž získáme 12, 0, 19, 17, 8, 23. Čísla pak takto

dosazuji do funkce

m, *a*: $(12, 0) \cdot \begin{pmatrix} 11 & 6 \\ 3 & 7 \end{pmatrix} = (12 \cdot 11 + 0 \cdot 3;\ 12 \cdot 6 + 0 \cdot 7) = (132; 72) \equiv_{Z26} (2, 20),$

t, *r*: $(19, 17) \cdot \begin{pmatrix} 11 & 6 \\ 3 & 7 \end{pmatrix} = (19 \cdot 11 + 17 \cdot 3;\ 19 \cdot 6 + 17 \cdot 7) = (260; 233) \equiv_{Z26} (0, 25),$

i, *x*: $(8, 23) \cdot \begin{pmatrix} 11 & 6 \\ 3 & 7 \end{pmatrix} = (8 \cdot 11 + 23 \cdot 3;\ 8 \cdot 6 + 23 \cdot 7) = (157, 209) \equiv_{Z26} (1, 1).$

Teď již převedeme číselné hodnoty na písmena „*CUAZBB*“ a zprávu máme ochráněnou před nežádoucími čtenáři.

Následné dešifrování provedeme pomocí inverzní matice. Nejprve vypočteme inverzní matici

$$\left(\begin{array}{cc|cc} 11 & 6 & 1 & 0 \\ 3 & 7 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{cc|cc} 11 & 6 & 1 & 0 \\ 0 & 3 & 21 & 1 \end{array}\right) \sim \left(\begin{array}{cc|cc} 11 & 0 & 11 & 24 \\ 0 & 3 & 21 & 1 \end{array}\right) \sim \left(\begin{array}{cc|cc} 1 & 0 & 1 & 14 \\ 0 & 1 & 7 & 9 \end{array}\right)$$ tudíž

$$H^{-1} = \begin{pmatrix} 1 & 14 \\ 7 & 9 \end{pmatrix}.$$

S touto inverzní matici dešifrujeme podle funkce $x = Y \cdot H^{-1}$ stejným způsobem jako jsme šifrovali

C, *U*: $(2, 20) \cdot \begin{pmatrix} 1 & 14 \\ 7 & 9 \end{pmatrix} = (2 \cdot 1 + 20 \cdot 7;\ 2 \cdot 14 + 20 \cdot 9) = (142; 208) \equiv_{Z26} (12, 0),$

A, *Z*: $(0, 25) \cdot \begin{pmatrix} 1 & 14 \\ 7 & 9 \end{pmatrix} = (0 \cdot 1 + 25 \cdot 7;\ 0 \cdot 14 + 25 \cdot 9) = (175; 233) \equiv_{Z26} (19, 17),$

B, *B*: $(1, 1) \cdot \begin{pmatrix} 1 & 14 \\ 7 & 9 \end{pmatrix} = (1 \cdot 1 + 1 \cdot 7;\ 1 \cdot 14 + 1 \cdot 9) = (8, 23) \equiv_{Z26} (8, 23).$

Příjemce zprávy opět převede výsledky na písmena a získá tak otevřený text.

3.4 Asymetrické metody šifrování

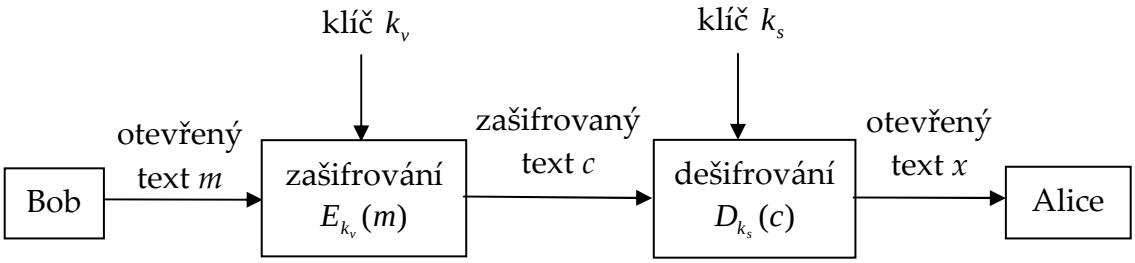
Metody asymetrického šifrování jsou založeny na principu jednosměrných funkcí využívající dvojicí klíčů a to **veřejný klíč** k_v a **soukromý klíč** k_s. Oba klíče jsou spolu jednoznačně svázány. Ze znalosti veřejného klíče je technicky prakticky nemožné vypočítat soukromý klíč. Veřejný klíč je volně dostupný například na serveru pro lidi, kteří tento klíč budou používat k zašifrování **otevřeného textu** *m*. Soukromý

klíč drží vlastník páru klíčů v tajnosti a použije ho k dešifrování **zašifrovaného textu** *c*. Neboli

$$E_{k_v}(m) = c$$

$$D_{k_s}(c) = m$$

$$D_{k_s}(E_{k_v}(m)) = m$$



Obrázek 3: Alice a Bob komunikují bezpečně

Většina v praxi využívaných algoritmů s veřejnými klíči jsou blokové šifry, jež se zprávou zacházejí jako se zprávou složenou z velkých celých čísel, přičemž bezpečnost jim zaručuje obtížnost řešení daného matematického problému. Nejznámější asymetrické šifry jsou ElGamal (autor: Taher ElGamal), RSA (autoři: Ronald Rivest, Adi Shamir, Leonard Adleman) a nakonec DSA (Digital Signature Algorithm jehož autorem je David W. Kravitz). [7]

3.4.1 RSA

V roce 1978 byl publikován algoritmus asymetrického šifrování RSA, který patří mezi nejužívanější algoritmy. Princip šifry spočívá v tom, že je jednoduché vypočítat hodnotu $n = p \cdot q$, kde p a q jsou prvočísla obsahující sto a více cifer, avšak při neznalosti obou prvočísel je technicky nerealizovatelné provést kanonický rozklad čísla n. U této šifry je veřejný klíč tvořen dvojicí hodnot $k_v = (e, n)$ a odpovídající soukromý klíč $k_s = (d, n)$, kde dvojice celočíselných hodnot e a d je jednoznačně určena, ale ze znalosti e a n je výpočetně téměř nemožné určit hodnotu d. Při šifrování systémem RSA se v praxi užívají klíče dlouhé 1024 bitů nebo 2048 bitů.

Otevřený text m je šifrován po blocích, jejichž hodnota je v binárním vyjádření menší než nějaké pevně dané přirozené číslo n. Z otevřeného textu m získáme

zašifrovaný blok textu *c*. Dále předpokládejme, že existují jednoznačně dané hodnoty *e* a *d*, pak **šifrovací funkce** je

$$c = m^e \pmod n,$$

a **dešifrovací funkce** je

$$m = c^d \pmod n.$$

Odesilatel zašifruje blok otevřeného textu m dle funkce $c = m^e \pmod n$, kde musí znát hodnoty veřejného klíče $k_v = (e, n)$. Stejným způsobem šifruje i ostatní bloky otevřeného textu a poté zašle zašifrovaný text adresátovi.

Příjemce dešifruje zašifrovaný blok textu c dle dle funkce $m = c^d \pmod n$, kde musí znát hodnoty soukromého klíče $k_s = (d, n)$.

Generování páru klíčů k_v, k_s

- Zvolíme dvě dostatečně velká prvočísla *p, q*.
- Vypočítáme součin $n = p \cdot q$.
- Určíme hodnotu $\varphi(n) = \varphi(p) \cdot \varphi(q) = (p-1) \cdot (q-1)$.
- Vybereme přirozené číslo *e* takové, pro které platí $NSD(\varphi(n), e) = 1$ a $1 < e < \varphi(n)$
- Učíme celé číslo *d* takové, aby platilo $e \cdot d \equiv 1 \bmod \varphi(n)$.
- Stanovíme veřejný klíč $k_v = (e, n)$.
- Stanovíme soukromý klíč $k_s = (d, n)$. [8]

Příklad 3.8

Pro názornost uvedeme příklad použití systému RSA. Záměrně zvolíme při generování páru klíčů malá prvočísla *p* a *q*. Při praktickém využití šifry je zapotřebí volit větší prvočísla.

- Zvolíme dvě prvočísla $p = 5$ a $q = 11$.
- Vypočítáme součin $n = p \cdot q = 5 \cdot 11 = 55$.
- Určíme hodnotu $\varphi(n) = \varphi(p) \cdot \varphi(q) = (p-1) \cdot (q-1) = 4 \cdot 10 = 40$
- Vybereme přirozené číslo *e* takové, aby bylo nesoudělné s $\varphi(n) = 40$ a menší než $\varphi(n)$. Této podmínce vyhovuje $e = 17$.

- Učíme celé číslo d takové, aby platilo $e \cdot d \equiv 1 \pmod{40}$. Hledanou hodnotu nalezneme např. Eukleidovým algoritmem $d = 33$, protože $17 \cdot 33 = 561 = 14 \cdot 40 + 1$.
- Máme veřejný klíč $k_v = (e, n) = (17; 55)$.
- Taktéž jsme obdrželi soukromý klíč $k_s = (d, n) = (33; 55)$.

Nyní zašifrujeme blok otevřeného textu *„dite“* pomocí veřejného klíče. Nejprve převedeme slovo *„dite“* do posloupnosti čísel dle Tabulky 2 v příloze. Dostaneme tak m = 3, 8, 19, 4 a ty zašifrujeme podle funkce $c = m^e \pmod{n}$

d: $3^{17} \pmod{55} = 129\,140\,163 \pmod{55} = 53 \pmod{55}$,

i: $8^{17} \pmod{55} = 2\,251\,799\,813\,685\,248 \pmod{55} = 13 \pmod{55}$,

t: $19^{17} \pmod{55} = 5\,480\,386\,857\,784\,802\,185\,939 \pmod{55} = 24 \pmod{55}$,

i: $4^{17} \pmod{55} = 17\,179\,869\,184 \pmod{55} = 49 \pmod{55}$,

tedy slovu *„dite“* odpovídá zašifrovaný blok $c = 53\,13\,24\,49$.

Přijemce obdrží zašifrovaný blok $c = 53\,13\,24\,49$ a dešifruje pomocí soukromého klíče $m = c^d \pmod{n}$

53: $53^{33} \pmod{55} = 3 \pmod{55}$,

13: $13^{33} \pmod{55} = 8 \pmod{55}$,

24: $24^{33} \pmod{55} = 19 \pmod{55}$,

49: $49^{33} \pmod{55} = 4 \pmod{55}$,

tedy po dešifrování obdržel příjemce původní blok otevřeného textu m = 3, 8, 19, 4, neboli text *„dite“*.

3.4.2 Útoky na systémy s veřejnými klíči

Zpracování kanonického rozkladu prošlo během posledních 30 let ohromným vývojem. Pokrok se odehrává jak na poli teoretickém, tak na poli technologickém. V roce 1970 bylo rozloženo na dvě prvočísla devětatřiceticiferné číslo. V té době byl podobný počin považován za něco fantastického. Když byla v roce 1978 poprvé publikována šifra RSA, byla jako součást studie zveřejněna i soutěž o rozklad 128ciferného čísla, přičemž vypsaná odměna měla hodnotu 100 dolarů. Jednalo se

o první takto navrženou odměnu – podobných projektů byla později celá řada. Požadované číslo bylo rozloženo na činitele až roku 1994, kdy se do práce zapojila celosvětová počítačová síť.

Při rozhodování o délce klíčů pro RSA je nutné vzít v potaz nejen Moorův zákon, ale také možný vývoj technik kanonického rozkladu. **Moorův zákon** říká, že každých 18 měsíců se výkon počítačů zdvojnásobí, aniž by se jakkoliv změnila jejich cena. Pro ilustraci můžeme uvést dramatický dopad nové matematické metody známé jako obecné síto číselných polí (GNFS) publikované roku 1993. Díky této metodě bylo možné zdroje určené pro rozklad čísla o určité velikosti využít k rozkladu výrazně větších čísel. Například zdroje, jež byly dříve zapotřebí pro rozklad čísla o 150cifrách, nyní stačí k rozkladu čísla o skoro 180cifrách. Tento pokrok v matematice výrazně převyšuje vliv technologického vývoje předpovídaného pro mnoho let dopředu.

Díky této metodě bylo roku 1999 rozloženo 155ciferné číslo RSA-512. Kanonický rozklad trval méně než 8 měsíců a opět se na ní podílela celosvětová počítačová síť. Pro ilustraci matematické složitosti tohoto problému uveďme, že v závěrečné fázi byla řešena soustava šesti miliónů rovnic! Následovala soutěž publikovaná v Knize kódů a šifer, ve které šlo také o faktorizaci 512bitového modula. Tyto rozklady na činitele mají velký význam, protože modula této velikosti (155 cifer či 512 bitů) byla ještě před několika lety běžně používaná v kryptografii veřejných klíčů.

V současné době se doporučuje, aby se velikost klíče RSA pohybovala v rozmezí 640–2048 bitů v závislosti na potřebném stupni zabezpečení. Číslo o 2048 bitech má v desítkové soustavě 617 cifer.

Jak by ovlivnil kryptoanalýzu možný vývoj kvantových počítačů? Ačkoliv by kvůli nim jistě muselo dojít k dramatickému nárůstu délky symetrických klíčů, těžko si představit, že by se tomu kryptografie nepřizpůsobila, a že by se symetrické algoritmy přestaly používat. U veřejných klíčů by situace mohla být jiná. Pro tyto systémy by totiž kvantové počítače představovali mnohem větší hrozbu. Například rozklad na prvočinitele by byl mnohem jednodušší. Naštěstí ani největší nadšenci pro kvantové počítače nepředpokládají, že by se tyto počítače začali používat v širší míře dříve než za 20 let. [3]

4 Závěr

Bezpečnost komunikace a obchodu v digitálním věku je cennější než mnohé nerostné poklady světa. Vývoj moderní kryptografie mapuje mnoho zajímavých metod z matematiky. Primárním úkolem této práce bylo seskupit několik zajímavých historických šifrovacích systémů a demonstrovat základní algebraické operace, především použití základů teorie dělitelnosti. Jelikož je kryptografie velice rozmanitým oborem a nelze v této práci obsáhnout vše, každý, kdo bude tuto práci chtít využít ať už při studiu či při výuce, ji může rozšířit o další zajímavé šifrovací metody.

Věřím, že tato práce bude přínosem nejen studentům předmětu informatiky v matematice, ale i pedagogům, kteří vyučují informatiku či matematiku na středních školách. Uplatnění matematických metod v tak zajímavém a rozmanitém oboru jako je kryptografie, může motivovat a rozvíjet studenty v dalším studiu matematiky.

5 Seznam použité literatury

[1] SINGH, Simon. Kniha kódů a šifer. Tajná komunikace od starého Egypta po kvantovou kryptografii. Praha: Dokořán a Argo, 2003. Český překlad: Petr Koubský a Dita Eckhardtová. ISBN 80-86569-18-7.

[2] MOLLIN, Richard A. An Introduction to Cryptography. Second Edition. Boca Raton: Chapman & Hall/CRC, 2007. ISBN-10: 1-58488-618-8.

[3] PIPER, Fred – MURPHY, Sean. Kryptografie. Průvodce pro každého. Vydání první, Praha: Dokořán, 2006. Český překlad: Pavel Mondschein.
ISBN 80-7363-074-5.

[4] KOUCKÝ, Miroslav. Matematika pro informatiky. (přednášky) FP TUL, Liberec, 2008/09.

[5] KOUCKÝ, Miroslav. Diskrétní matematika II. Skripta TUL, Liberec, 2004.

[6] HANKERSON, Darrel R. et al. Coding Theory and Cryptography. Second Edition. New York: Marcel Dekker, 2000. ISBN 0-8247-0465-7.

[7] SALOMAA, Arto. Public-Key Cryptography. Second Edition. Berlin: Springer-Verlag, 1996. ISBN 3-540-61356-0.

[8] MLÝNEK, Jaroslav. Zabezpečení obchodních informací. Vydání první, Brno, Computer Press, 2007. ISBN 978-80-251-1511-4.

6 Seznam příloh

Příloha č. 1 – Tabulky

Příloha č. 2 – Sbírka úloh

Příloha č. 3 – Příklad Vigenèrovy šifry v C++

Příloha č. 1 – Tabulky

Tabulka 1: Vigenèrův čtverec

a	***b***	***c***	***d***	***e***	***f***	***g***	***h***	***i***	***j***	***k***	***l***	***m***	***n***	***o***	***p***	***q***	***r***	***s***	***t***	***u***	***v***	***w***	***x***	***y***	***z***
B	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*	*A*
C	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*	*A*	*B*
D	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*	*A*	*B*	*C*
E	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*	*A*	*B*	*C*	*D*
F	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*	*A*	*B*	*C*	*D*	*E*
G	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*	*A*	*B*	*C*	*D*	*E*	*F*
H	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*	*A*	*B*	*C*	*D*	*E*	*F*	*G*
I	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*	*A*	*B*	*C*	*D*	*E*	*F*	*G*	*H*
J	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*	*A*	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*
K	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*	*A*	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*
L	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*	*A*	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*
M	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*	*A*	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*
N	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*	*A*	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*
O	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*	*A*	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*
P	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*	*A*	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*
Q	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*	*A*	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*
R	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*	*A*	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*
S	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*	*A*	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*
T	*U*	*V*	*W*	*X*	*Y*	*Z*	*A*	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*
U	*V*	*W*	*X*	*Y*	*Z*	*A*	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*
V	*W*	*X*	*Y*	*Z*	*A*	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*
W	*X*	*Y*	*Z*	*A*	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*
X	*Y*	*Z*	*A*	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*
Y	*Z*	*A*	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*
Z	*A*	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*
A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*

Tabulka 2: Pořadí znaků (mod 26)

a	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*j*	*k*	*l*	*m*	*n*	*o*	*p*	*q*	*r*	*s*	*t*	*u*	*v*	*w*	*x*	*y*	*z*
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Příloha č. 2 – Sbírka úloh

Příklad 6.1

Pomocí kanonických rozkladů čísel *a*, *b* nalezněte:

a) NSD(*a*,*b*), kde *a* = 467 313, *b* = 1 708 245

b) NSN(*a*,*b*), kde *a* = 8 245, *b* = 1 171.

Příklad 6.2

Nalezněte všechna řešení kongruence $ax \equiv b(m)$, kde *a* = 272, *b* = 28, *c* = 516. Výsledek vyjádřete v soustavě nejmenších nezáporných zbytků modulo *m*.

Příklad 6.3

Nalezněte všechna řešení kongruence $561x + 51 \equiv 0 \pmod{234}$. Výsledek vyjádřete v soustavě nejmenších nezáporných zbytků modulo 234.

Příklad 6.4

V symetrické grupě S_6 vypočtěte:

a) součin $\pi \cdot \rho$,

b) součin $\rho \cdot \pi^{-1}$,

kde $\pi = \begin{pmatrix} 1\,2\,3\,4\,5\,6 \\ 3\,1\,2\,6\,4\,5 \end{pmatrix}$, $\rho = \begin{pmatrix} 1\,2\,3\,4\,5\,6 \\ 3\,4\,5\,1\,6\,2 \end{pmatrix}$.

Příklad 6.5

Použijte jednoduchou transpoziční šifru s klíčem $\pi = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 5\,1\,4\,3\,2 \end{pmatrix}$.

a) Zašifrujte text „*stavebni sporeni*“.

b) Dešifrujte text „*ANTFAVJELEINSJE*“.

Příklad 6.6

Uvažujte permutace $\pi, \rho \in S_5$, kde $\pi = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 4\,3\,2\,5\,1 \end{pmatrix}$ a $\rho = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 2\,1\,3\,5\,4 \end{pmatrix}$.

a) Vypočtěte součin $\pi \cdot \rho$.

b) Dešifrujte text „*OFSRIJNVIAAAEBZZXVYA*“.

Příklad 6.7

Uvažujte Caesarova šifra s posunem o tři místa.

a) Zašifrujte text „*galske valky*“.

b) Dešifrujte text „*YRMHYXGFH*“.

Příklad 6.8

Použijte jednoduchou substituci s klíčovou větou „*nekonecny pribeh*“.

a) Zašifrujte text „*sejdeme se v pet pod lipou*“.

b) Dešifrujte text „*MNOCBIJGOHNQSNFCD*“.

Příklad 6.9

Uvažujte afinní šifrování s klíčem (*a*, *b*) = (17, 11).

a) Zašifrujte text „*dobyti raje*“.

b) Dešifrujte text „*ZODFWPSZPQNHCNF*“.

Příklad 6.10

Uvažujte afinní šifrování s klíčem (*a*, *b*) = (11, 20).

a) Zašifrujte text „*zemetreseni*“.

b) Dešifrujte text „*VSZHUBS*“.

Příklad 6.11

Použijte Vigenèrovu šifru s klíčovým slovem „*krasny*“.

a) Zašifrujte text „*kyselina benzoova*“.

b) Dešifrujte text „*VVCZVDPIEAABOTHASDBRBDR*“.

Příklad 6.12

Použijte Vigenèrovu šifru s klíčovým slovem *„hasic“*.

a) Zašifrujte text *„odvazlivec“*.

b) Dešifrujte text *„KAJMFLVAT“*.

Příklad 6.13

Uvažujte Hillovo šifrování s klíčem $H = \begin{pmatrix} 19 & 10 \\ 5 & 1 \end{pmatrix}$.

a) Zašifrujte text *„delo“*.

b) Dešifrujte text *„LOCAXI“*.

Příklad 6.14

Uvažujte Hillovo šifrování s klíčem $H = \begin{pmatrix} 7 & 18 \\ 10 & 17 \end{pmatrix}$.

a) Zašifrujte text *„kolo“*.

b) Dešifrujte text *„QGXE“*.

Příklad 6.15

Pomocí RSA metody

a) zašifrujte text *„rivest“*, máte-li veřejný klíč $k_v = (e, n) = (5; 119)$

b) dešifrujte zprávu *m* = 86, 28, 0, 3, 43, 68, máte-li soukromý klíč $k_s = (d, n) = (77; 119)$.

Řešení k úlohám

6.1 a) 3 927 b) 9 654 895

6.2 $x \equiv 2; 131; 260; 389 \pmod{516}$

6.3 $x \equiv 7; 85; 163 \pmod{234}$

6.4 a) $\pi \cdot \rho = \begin{pmatrix} 1\,2\,3\,4\,5\,6 \\ 5\,3\,4\,2\,1\,6 \end{pmatrix}$ b) $\rho \cdot \pi^{-1} = \begin{pmatrix} 1\,2\,3\,4\,5\,6 \\ 1\,5\,6\,2\,4\,3 \end{pmatrix}$

6.5 a) „*ESVATPBSINIONER*“ b) „*nafta je levnejsi*“

6.6 a) $\pi \cdot \rho = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 5\,3\,1\,4\,2 \end{pmatrix}$ b) „*sifrovani je zabava*“

6.7 a) „*JDOVNHYDONB*“ b) „*vojevudce*“

6.8 a) „*QCBOCDCQCUJCSJGOAIJGT*“ b) „*radeji pod kastanem*“

6.9 a) „*KPCDWROLIB*“ b) „*Krystof Kolumbus*“

6.10 a) „*JMWMVZMKMHE*“ b) „*tornado*“

6.11 a) „*UPSWYGXRBWAXFVS*“ b) „*le chiffre indechiffrable*“

6.12 a) „*VDNIBSINME*“ b) „*daredevil*“

6.13 a) „*ZITU*“ b) „*raketa*“

6.14 a) „*CCJU*“ b) „*okno*“

6.15 a) m = 68, 43, 21, 72, 86, 66 b) „*Shamir*“

Příloha č. 3 – Příklad Vigenèrovy šifry v C++

```
#include <iostream>
#include <stdlib.h>
#include <string.h>
using namespace std;

int main(void)
{
    string keyword;
    string message;
    string theend;
    int keylen;
    int meslen;
    int crypted;
    int i=0;

    cout << "VIGENEROVA SIFRA\n==================\n\n";
    cout << "Napiste klic : ";
    getline( cin, keyword );

    cout << "Napiste zpravu : ";
    getline( cin, message );

    keylen = keyword.length();
    meslen = message.length();

    addkeyword:
    if ( keylen < meslen ) {
         keyword = keyword + keyword;
         keylen = keyword.length();
         if ( keylen < meslen ) goto addkeyword;
    }
    cout << "Zasifrovany text : ";
    while ( i < meslen ) {
          keyword[i] -= 'a';
          if ( ( message[i] + keyword[i]) > 'z' )
```

```
            crypted = keyword[i] + message[i] - 26;
          else if ( message[i] == 32 ) crypted = message[i];
          else crypted = message[i] + keyword[i];
          cout << (char)crypted;
          i++;
    }
    cout << "\nOpakovat (a/n)? : ";
    getline( cin, theend );
    if ( theend[0] == 'a' ) main();
    return 0;
}
```